

Smartphones e Tablets

Autora: Matilde Francisco n.º 17 7.º B

Introdução

Atualmente, as tecnologias fazem parte do nosso dia a dia tornando-se um equipamento essencial.

Um smartphone está equipado com software que permite a utilização de leitores de música e vídeo, navegador de internet, serviços de chat, chamadas e vídeo chamadas pela Internet em tempo real.

Ainda que existam vários sistemas operativos (IOS, Android, Blackberry, Symbian, Windows Phone, etc), todos os smartphones funcionam de forma semelhante e oferecem o mesmo tipo de serviços.



Perigos existentes

Um smartphone ou tablet, tal como os computadores, é vulnerável a certos perigos, como o phishing, SPAM, malware, roubo de identidade ou informação pessoal.

Tal como no computador, quando um smartphone ou tablet fica infetado é possível detetar uma diminuição na sua performance, o aparecimento de aplicações que não foram instaladas pelo utilizador, a alteração de configurações no telemóvel e uma diminuição drástica no tempo de vida útil da bateria.



Perigos existentes

Alguns dos vírus que se encontram nos telemóveis têm como objetivo o roubo de palavras-passe dos utilizadores, autenticações bancárias, ou mesmo envio de mensagens e chamadas para números de valor. Para além dos riscos associados à invasão do sistema do smartphone, existem os riscos associados à receção e envio de mensagens com conteúdo inapropriado ou violento, dando origem a questões como o sexting e o Image do livro.



Prevenção

Proteger o nosso telemóvel com uma password.

Ativar o autobloqueio para quando o telemóvel está inactivo.

Nunca fazer download de aplicações fora dos mercados próprios dos sistemas operativos.

Evitar dar o número de telefone a desconhecidos ou disponibilizá-lo na Internet.



Prevenção

Utilizar um antivírus no nosso telemóvel e fazer análises regulares ao conteúdo do smartphone;

Manter o bluetooth desligado e utilizar apenas quando necessário;

Instalar software de limpeza remota de smartphones.

Aplicações como o Find My Phone ou o Android Device Manager da Google permitem localizar o nosso telemóvel remotamente apagar tudo o que tem dentro, em caso de roubo;



Prevenção

Não utilizar a aplicação de notas para guardar informação sensível como passwords, dados bancários ou outro tipo de informação pessoal é um dos locais onde os ladrões de informação procuram em primeiro lugar;

Bibliografia

www.internetsegura.pt